UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF CALIFORNIA

JUSTM2J LLC,

Plaintiff,

v.

AYDEN BREWER, et al.,

Defendants.

No. 2:25-cv-00380-DAD-SCR

ORDER DENYING PLAINTIFF'S MOTION FOR TEMPORARY RESTRAINING ORDER WITHOUT PREJUDICE AND GRANTING IN PART PLAINTIFF'S MOTION FOR EXPEDITED DISCOVERY

(Doc. No. 2)

This matter is before the court on plaintiff's *ex parte* motion for a temporary restraining order and plaintiff's motion for expedited discovery. (Doc. No. 2.) For the reasons explained below, the court will deny plaintiff's motion for a temporary restraining order and will grant in part plaintiff's motion for expedited discovery.

BACKGROUND

On January 27, 2025, plaintiff JustM2J LLC initiated this fraud action against named defendants Ayden Brewer, Jon Litz, and Jason St. George, and unknown defendant John Doe 1. (Doc. No. 1.) In its complaint, plaintiff alleges the following.

Plaintiff is a Delaware limited liability company that is the assignee of all claims belonging to Nakamoto LLC related to a series of cyber-attacks ("the Bittensor attacks") against the participants of Bittensor. (*Id.* at ¶¶ 1, 10.) Nakamoto LLC, as the assignor of plaintiff,

/////

purportedly lost approximately $13,000,000 in crypto assets as a result of the Bittensor attacks.[1] (*Id.* at ¶ 6.) Bittensor is a decentralized network that is designed to foster collaboration and competition among AI researchers. (*Id.* at ¶ 21.) It does this by allowing participants to earn rewards in the form of a digital token called TAO for providing computations and machine learning models aimed at completing certain tasks, such as image recognition. (*Id.*) Bittensor is open-source in that its source code is freely available to the public. (*Id.*) To participate in Bittensor, participants must have a piece of software called a wallet which enables them to receive, store, and transfer TAO and a private key that allows a user to access and control a wallet and its contents. (*Id.* at ¶ 24.) Defendant St. George was an employee of Opentensor Foundation ("Opentensor"), which maintains, develops, and improves Bittensor. (*Id.* at ¶¶ 25, 27.) During his tenure there, defendant St. George had access to Opentensor's proprietary key which allowed access to Opentensor's PyPI account.[2] (*Id.* at ¶ 27.) Defendants Brewer, St. George, Litz, and John Doe 1 entered into an agreement to plan and execute the Bittensor attacks around April of 2024. (*Id.* at ¶ 28.) On May 20, 2024, defendants registered a domain named opentensor.io which appeared as though it belonged to Opentensor. (*Id.* at ¶ 29.)

On May 22, 2024, Opentensor released an upgrade to Bittensor's software called version 6.12.2. (*Id.* at ¶ 30.) This release first took place on Github, which is an open-source code repository that Opentensor uses for Bittensor. (*Id.*) This release was also intended to be published on PyPI by Opentensor. (*Id.* at ¶ 31.) However, defendants used the proprietary Opentensor key to upload a malicious version of the Bittensor update. (*Id.*) This prevented the upload of the legitimate version 6.12.2 of Bittensor to PyPI by Opentensor. (*Id.*) Bittensor users who downloaded version 6.12.2 from PyPI prior to July 2, 2024, therefore received a malicious

---

[1] Neither in its complaint nor in the pending *ex parte* motion for a temporary restraining order does plaintiff address how or why Nakamoto LLC assigned its claims in this regard to plaintiff nor does plaintiff explain the nature of the relationship between itself and Nakamoto LLC.

[2] Plaintiff's allegations with respect to the PyPI account are vague and unclear. It may be that plaintiff is attempting to allege that Opentensor has an account on PyPI that it uses to upload updates to its Bittensor software as packages and that defendants improperly gained access to the login credentials for that account.

version of the update which executed the same functions but also intercepted private keys associated with the wallets of those users and sent those keys to opentensor.io. (*Id.* at ¶ 33.) On May 30, defendants used one private key obtained in this manner to steal a total of 1039.9 TAO from the wallets of one user, amounting to roughly $480,000. (*Id.* at ¶ 35.) On June 1, defendants used a different private key obtained in this manner to steal a total of 28,368 TAO from Nakamoto's wallet, amounting to roughly $13,000,000. (*Id.* at ¶ 36.) On July 2, defendants transferred 32,395 TAO, valued at approximately $15,000,000, from the wallets of 30 users. (*Id.* at ¶ 37.)

Opentensor then placed the Bittensor network in safe mode and on July 3 discovered that the malicious version that had been uploaded to PyPI. (*Id.* at ¶¶ 38, 39.) A series of transfers and exchanges occurred which caused the assets taken in these three attacks to be deposited into specific wallet addresses ("the Destination Addresses") across several exchanges. (*Id.* at ¶¶ 41, 42.) Plaintiff does not allege when these transfers occurred. Opentensor retained a forensic investigator and contacted law enforcement regarding the Bittensor attacks, though plaintiff does not allege when the investigation conducted by the forensic investigator was completed. (*Id.* at ¶ 40.) Plaintiff has provided a declaration attached to its *ex parte* motion for a temporary restraining order which states that the forensic investigator was hired in July 2024. (Doc. No. 2-2 at ¶ 6.)

Assets from the May 30 cyberattack, amounting to 1030.9 TAO, were transferred to the TAO-wTAO bridge which allows users to convert TAO to wTAO, a separate cryptocurrency. (Doc. No. 1 at ¶ 43.) Those wTAO assets were then converted to Ethereum ("ETH"), a separate cryptocurrency, and deposited into the following cryptocurrency wallet addresses:

Cryptocurrency and Volume	Destination Address	Address Type	USD Value[3]
103 ETH	0x5e92aB69eB102cFC4A7 C507D8Dc3cC1eEdE25Eb0	WhiteBit Deposit	$412,206

[3] Plaintiff represents that the value of the funds located in each of the destination addresses listed in this order were calculated using the peak ETH/USD conversion rate over the past thirty (30) days. (Doc. No. 1 at 9 n.1.)

Cryptocurrency and Volume	Destination Address	Address Type	USD Value[3]
		Address	
.884 ETH	0x09F76d4FC3bcE5bF2854 3F45c4CeE9999E0a0AAf	June 1, 2024 Hack Address	$3,537

(*Id.* at ¶ 46.)[4]

According to plaintiff, assets from the June 1 attack, amounting to 28,368 TAO, were transferred to the TAO-wTAO bridge and temporarily deposited to the wallet address identified as the traced endpoint for the .884 ETH taken in the May 30 attack. (*Id.* at ¶ 47.) Those wTAO assets were then exchanged for ETH, wETH, a separate cryptocurrency, and USD Coin. (*Id.* at ¶ 48.) USD Coin is a stablecoin cryptocurrency designed to maintain a 1:1 conversion rate with USD. (*Id.* at 9 at n.2.) Those assets were then distributed over several deposit addresses in Binance, WhiteBit, and HTX, which are exchanges used to store and trade cryptocurrencies. (*Id.* at ¶ 49.) Approximately 1,205 ETH from those assets was routed through the Railgun Privacy Protocol, which is a system designed to hide the details of cryptocurrency transactions. (*Id.* at ¶ 51.) Plaintiff claims that 1,055 ETH was transferred from the Railgun Privacy Protocol to the Synapse Protocol bridge, a tool used to transfer cryptocurrency assets between different blockchains, and then transferred to a variety of cryptocurrency exchanges while the remaining 150 ETH was sent to two specific deposit addresses. (*Id.* at ¶¶ 52, 53.) The mixture of assets obtained as a result of the June 1 attack, according to plaintiff, reached the following ending wallet addresses:

Cryptocurrency and Volume	Destination Address	Address Type	USD Value
395,301 USDC	0x8f3100AD91cbfbE8aA58 845083B25249f8FfdB29	Binance Deposit Address	$395,301
197,336 USDC	0x9C6D589B7e6Cea55138A 3ea1E0AC615126290ED2	Binance Deposit Address	$197,336

[4] Though plaintiff alleges that the value of the assets taken amounted to approximately $480,000, the amount in the Destination Addresses listed only adds up to $415,743. Plaintiff does not clarify this discrepancy in its complaint.

Cryptocurrency and Volume	Destination Address	Address Type	USD Value
99.9999 ETH	0x9C6D589B7e6Cea55138A 3ea1E0AC615126290ED2	Binance Deposit Address	$396,198
98.9997 ETH	0x6C030fCf0529baa3FB655 32a25aB5154BBE335cB	WhiteBit Deposit Address	$396,157
384,192 USDC	0x5625f748FF2E0784744a4 F974d173924D7219097	WhiteBit Deposit Address	$384,192
63.9997 ETH	0x047050a2A09dc27f23Df5 19dF7D19074A6a3343f	WhiteBit Deposit Address	$256,087
153.9994 ETH	0x15a8130D8F8AcD474486 7b3D51491D1e0189f908	WhiteBit Deposit Address	$616,267
86.9996 ETH	0x65a7437f2F6EF3c203b19 af8f1787Db03F1FB20B	WhiteBit Deposit Address	$348,133
24.9995 ETH	0x954f0dF9B7555a755CFd8 55Bf4809c4e15b732B0	WhiteBit Deposit Address	$100,009
25 ETH	0x6d5f108E94718e346C5eC 1C52cE7edd5cDD1a89A	WhiteBit Deposit Address	$100,050
20 ETH	0xe6a2aAE8811c20869a900 2A808b7c31a0786588E	WhiteBit Deposit Address	$80,040
28.9 ETH	0xBc9b0B672f8941109Ff37 831fa43c922B0935d17	WhiteBit Deposit Address	$115,657
24.9997 ETH	0x56DbE5de6a37f23e85DA 00338e1dd58216a40b6c	HTX Deposit Address	$100,009
99.9996 ETH	0x3A9EDb8C26c61F816De AcE92764964bb1483456E	HTX Deposit Address	$396,198
63.9998 ETH	0x58A6cfc6D9b00E78056f6 2D8a1efa54741AcEe01	HTX Deposit Address	$256,087
74.9998 ETH	0x01d2B465d5ba513387932 290fe1a1644d5A83F22	HTX Deposit Address	$300,145
77.9998 ETH	0x80839E957F5BC7D72e71 626636C5FAE202B758e7	HTX Deposit Address	$312,151
99.9996 ETH	0x8C227480B8F9E894a572 687799FE5368622FCDC1	HTX Deposit Address	$396,198
85.9997 ETH	0x7824ee032bd857FbbDd9e 351F50F5eB80b0ADB13	HTX Deposit Address	$344,167

Cryptocurrency and Volume	Destination Address	Address Type	USD Value
99.9999 ETH	0x6BEe51F3cf378Fc167DFeeF1ea2c856ce6Ec12d8	KuCoin Deposit Address	$396,198
99.9999 ETH	0x3898879e531D2ce92d8FB23cb7aD86d5472060C1	KuCoin Deposit Address	$396,198
1.999904 ETH	0xb3C7E5E8F138F23C461C941AF133BC14F863285E	KuCoin Deposit Address	$7,999
19.9998 ETH	0x95034c37c1C1D8484089Fb46889932402DCA0F82	KuCoin Deposit Address	$80,035
9.999985 ETH	0x85De72B97d6eFe7bFCDaC472fA182F79Da8619DC	KuCoin Deposit Address	$40,015
9.99987 ETH	0x91aC15FE89315867F8BDd7b5bB40D450E2fF0320	KuCoin Deposit Address	$40,015
4.999909 ETH	0x9f02577718bA0505DbB07a13eCc38d809b13399a	KuCoin Deposit Address	$20,005
50 ETH	0x26658c8e719268e473491E26E5a33e284d1Ea4bF	MexC Deposit Address	$200,100
50 ETH	0xC49BDbD2F3ed50cD095B108bca6bd7596F2D4ba7	EXCH.CX Deposit Address	$200,100
35 ETH	0xD66766E43cB66628478Ed9D12d076849e81fDfF5	EXCH.CX Deposit Address	$140,070
228 ETH	0x85E14ec0E976414EDE6B38A0b5E5B7879290EF53	EXCH.CX Deposit Address	$912,456
100 ETH	0xCAec170151ABaED4Fc3a158a7c3f78889C0dD9e5	EXCH.CX Deposit Address	$400,200
20 ETH	0xDcDEA8a8cAB06958C590E64937c0D4853744c335	EXCH.CX Deposit Address	$80,040
14.9999 ETH	0x356E2Df6a43A26E340Dae0C3649c26aCcf384082	EXCH.CX Deposit Address	$59,989
10.0001 ETH	0x686Fa4976D8C7EA5BCAc53EB86ea453c44f7c5f3	EXCH.CX Deposit Address	$40,020
9.999857 ETH	0x79Ce9C4160F4AAf5191fC516511c78D0dd24e885	EXCH.CX Deposit Address	$40,015
9.999908 ETH	0x08e637130C4eFBb4e48DC13Cc95c7fC6355A3BdB	EXCH.CX Deposit Address	$40,015

Cryptocurrency and Volume	Destination Address	Address Type	USD Value
4.999893 ETH	0x34A64406Eb3FBc18994C 7B2827E5D266671d011D	EXCH.CX Deposit Address	$20,005
4.999963 ETH	0x22Cb8d3A6D43F86DCB E751e4a2cf235ba1312b79	EXCH.CX Deposit Address	$20,005
4.999964 ETH	0x16929803A0F2392497C8 1404d7748c65ff9C0c2a	EXCH.CX Deposit Address	$20,005
4.999968 ETH	0x0eC0AC79148305FE8177 45C18c0aF4Ba07547B98	EXCH.CX Deposit Address	$20,005
4.99995 ETH	0xF239a90A91e4598b541D7D78bea E3621193b9c9D	EXCH.CX Deposit Address	$20,005
4.999953 ETH	0x292685ac52Bdb8fa08aCB 50Da3801bd87C4137AF	EXCH.CX Deposit Address	$20,005
4.999963 ETH	0xFF506cD2A2bFDFA80EF 62DC22839E16ce40CA4F5	EXCH.CX Deposit Address	$20,005
4.999968 ETH	0xA4F75e61cdAd561bdDD 35e921288bd60002f9633	EXCH.CX Deposit Address	$20,005
4.999952 ETH	0x7DA771ec163C461adec0 9ED2D88f2A5ec62Ff13D	EXCH.CX Deposit Address	$20,005
4.99986 ETH	0xbaE5d5c76c42D93CE658 28E9B0c86458Dc5329A7	EXCH.CX Deposit Address	$20,005
4.999851 ETH	0x18c7278D515EF9601191 48a0c5228718281fC312	EXCH.CX Deposit Address	$20,005
9.9999 ETH	0xfffDEc00c2DD485bFfEde c4eF65489D1F076E1a1	Exolix Deposit Address	$40,015
49.999678 ETH	0x47713cb34FAbd63b39D7 C5c6f675dCa39d22762B	Unnamed Service	$200,095
1.999818 ETH	0x47713cb34FAbd63b39D7 C5c6f675dCa39d22762B	Unnamed Service	$7,999
.999823 ETH	0x47713cb34FAbd63b39D7 C5c6f675dCa39d22762B	Unnamed Service	$3,997
277,906 USDC	0xFA7093CDD9EE6932B4e b2c9e1cde7CE00B1FA4b9	Railgun.ch Privacy Protocol	$277,906
22.41 wETH	0xFA7093CDD9EE6932B4e b2c9e1cde7CE00B1FA4b9	Railgun.ch Privacy Protocol	$97,688
10 ETH	0x252262813114eB1FF5261 E2408B39410a5a8dCCB	Link Address	$40,020

Cryptocurrency and Volume	Destination Address	Address Type	USD Value
300,000 USDC	0xd5960CA93A0b3fEE31a6 B691BCA27e5C36701B83	Coinbase Deposit Address	$300,000

(*Id.* at ¶ 54.)[5]

In addition according to plaintiff, assets from the July 2 attack, amounting to 32,395 TAO, were consolidated in a single Bittensor wallet. (*Id.* at ¶ 55.) Those assets were then transferred to a KuCoin or MexC deposit address, both of which are separate cryptocurrency exchanges, or routed through the TAO-wTAO bridge to the Railgun Privacy Protocol, at which point the assets became untraceable. (*Id.* at ¶¶ 51, 55, 56.) The last known location of those assets are the following deposit addresses:

Cryptocurrency and Volume	Destination Address	Address Type	USD Value
8,295 TAO	5CrmVKApX6sJybZaL1geHfz vHWeCpbavqrrXgYLCQmheh X2q	KuCoin	$4,587,135
11,100 TAO	5FqBL928choLPmeFz5UVAv onBD5k7K2mZSXVC9RkFzL xoy2s	MexC	$6,105,000
333.621 ETH	0xFA7093CDD9EE6932B4eb 2c9e1cde7CE00B1FA4b9	Railgun.ch Privacy Protocol	$1,335,151

(*Id.* at ¶ 57.)[6]

Based upon these allegations, plaintiff asserts seven claims against the defendants: (1) accessing protected computers without authorization and causing damage or loss in violation of the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(a)(2)(C), 1030(a)(4) and 1030(a)(5)(C); (2) intercepting electronic communications by Bittensor participants in violation of the Wiretap Act, 18 U.S.C. § 2510, *et seq.*; (3) fraud; (4) conversion; (5) unjust enrichment; (6) imposition of

[5] Though plaintiff alleges that the value of the assets taken amounted to approximately $13,000,000, the amount in the Destination Addresses adds up only to $9,659,612. Plaintiff also does not clarify this discrepancy in its complaint.

[6] Though plaintiff alleges that the value of the assets taken amounted to approximately $15,000,000, the amount in the Destination Addresses adds up only to $12,027,286. Plaintiff also does not clarify this discrepancy in its complaint.

a constructive trust and disgorgement of funds; and (7) possession of stolen property in violation of California Penal Code § 496. (Doc. No. 1 at ¶¶ 71–113.)

Plaintiff filed the pending *ex parte* motion for a temporary restraining order with its complaint. (Doc. No. 2.) In that *ex parte* motion, plaintiff seeks an order from this court freezing accounts that received allegedly stolen digital assets, including the assets held in the Destination Addresses of the assets taken in the Bittensor cyberattacks, and other related digital accounts maintained by defendants purportedly in order to preserve the *status quo* during the litigation of this action. (Doc. No. 2-1 at 7.) Defendants also request authorization to conduct limited expedited discovery to identify the "John Doe" defendant(s) and confirm the location of stolen assets. (*Id.* at 7.)

LEGAL STANDARD

A. Temporary Restraining Order

The standard governing the issuing of a temporary restraining order is "substantially identical" to the standard for issuing a preliminary injunction. *See Stuhlbarg Int'l Sales Co. v. John D. Brush & Co.*, 240 F.3d 832, 839 n.7 (9th Cir. 2001). "The proper legal standard for preliminary injunctive relief requires a party to demonstrate 'that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest.'" *Stormans, Inc. v. Selecky*, 586 F.3d 1109, 1127 (9th Cir. 2009) (quoting *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008)); *see also Ctr. for Food Safety v. Vilsack*, 636 F.3d 1166, 1172 (9th Cir. 2011) ("After *Winter*, 'plaintiffs must establish that irreparable harm is likely, not just possible, in order to obtain a preliminary injunction.'"); *Am. Trucking Ass'ns v. City of Los Angeles*, 559 F.3d 1046, 1052 (9th Cir. 2009). A plaintiff seeking a preliminary injunction must make a showing on all four of these prongs. *All. for the Wild Rockies v. Cottrell*, 632 F.3d 1127, 1135 (9th Cir. 2011). The Ninth Circuit has also held that "[a] preliminary injunction is appropriate when a plaintiff demonstrates . . . that serious questions going to the merits were raised and the balance of hardships tips sharply in the plaintiff's favor." *Id.* at 1134–35 (quoting

/////

Lands Council v. McNair, 537 F.3d 981, 987 (9th Cir. 2008) (*en banc*)).[7] The party seeking the injunction bears the burden of proving these elements. *Klein v. City of San Clemente*, 584 F.3d 1196, 1201 (9th Cir. 2009); *see also Caribbean Marine Servs. Co. v. Baldrige*, 844 F.2d 668, 674 (9th Cir. 1988) (citation omitted) ("A plaintiff must do more than merely allege imminent harm sufficient to establish standing; a plaintiff must *demonstrate* immediate threatened injury as a prerequisite to preliminary injunctive relief."). Finally, an injunction is "an extraordinary remedy that may only be awarded upon a clear showing that the plaintiff is entitled to such relief." *Winter*, 555 U.S. at 22.

Relevant to the court's consideration of plaintiff's pending *ex parte* motion, a court may only issue a temporary restraining order without notice to the adverse party when:

> (A) specific facts in an affidavit or a verified complaint clearly show that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition [and] (B) the movant's attorney certifies in writing any efforts made to give notice and the reasons why it should not be required.

Fed. R. Civ. P. 65(b)(1). Moreover, *ex parte* temporary restraining orders "should be restricted to serving their underlying purpose of preserving the *status quo* and preventing irreparable harm just so long as is necessary to hold a hearing, and no longer." *Granny Goose Foods, Inc. v. Bhd. of Teamsters & Auto Truck Drivers Loc. No. 70 of Alameda Cnty.*, 415 U.S. 423, 439 (1974).

B. Expedited Discovery

Federal Rule of Civil Procedure Rule 26(d) provides that no discovery can be sought "from any source before the parties have conferred as required by Rule 26(f), except . . . when authorized . . . by court order." Fed. R. Civ. P. 26(d)(1). Generally, courts require a showing of good cause to permit expedited discovery. *In re Countrywide Fin. Corp. Derivative Litig.*, 542 F. Supp. 2d 1160, 1179 (C.D. Cal. 2008), *abrogated on other grounds by United States v. State*

[7] The Ninth Circuit has found that this "serious question" version of the circuit's sliding scale approach survives "when applied as part of the four-element *Winter* test." *All. for the Wild Rockies*, 632 F.3d at 1134. "That is, 'serious questions going to the merits' and a balance of hardships that tips sharply towards the plaintiff can support issuance of a preliminary injunction, so long as the plaintiff also shows that there is a likelihood of irreparable injury and that the injunction is in the public interest." *Id.* at 1135.

Water Res. Control Bd., 988 F.3d 1194, 1205 (9th Cir. 2021); *Criswell v. Boudreaux*, No. 1:20-cv-01048-DAD-SAB, 2020 WL 5235675, at *25 (E.D. Cal. Sept. 2, 2020). "Good cause may be found where the need for expedited discovery, in consideration of the administration of justice, outweighs the prejudice to the responding party." *Semitool, Inc. v. Tokyo Electron Am., Inc.*, 208 F.R.D. 273, 276 (N.D. Cal. 2002). In determining whether good cause exists, courts consider: "(1) whether a preliminary injunction is pending; (2) the breadth of the discovery request; (3) the purpose for requesting the expedited discovery; (4) the burden on the defendants to comply with the requests; and (5) how far in advance of the typical discovery process the request was made." *Rovio Ent. Ltd. v. Royal Plush Toys, Inc.*, 907 F. Supp. 2d 1086, 1099 (N.D. Cal. 2012).

Applying the test set forth in *Semitool*, California district courts have found good cause to authorize expedited discovery to ascertain the identity of an unknown defendant. *See, e.g.*, *AF Holdings LLC v. Doe*, No. 2:12-cv-02207-KJM-DAD, 2012 WL 6608993, at *1 (E.D. Cal. Dec. 18, 2012) (granting leave to conduct expedited discovery to determine the identity of a Doe defendant in a copyright infringement action); *First Time Videos, LLC v. Doe*, No. 2:12-cv-00621-GEB-EFB, 2012 WL 1355725 (E.D. Cal. Apr. 18, 2012) (same); *UMG Recordings, Inc. v. Doe*, No. 08-cv-03999-RMW, 2008 WL 4104207 (N.D. Cal. Sept. 4, 2008) (same); *Arista Recs. LLC v. Does 1–43*, No. 07-cv-02357-LAB-POR, 2007 WL 4538697 (S.D. Cal. Dec. 20, 2007) (same). Moreover, the Ninth Circuit has held that "'where the identity of the alleged defendant[ ] [is] not [ ] known prior to the filing of a complaint[,] the plaintiff should be given an opportunity through discovery to identify the unknown defendants, unless it is clear that discovery would not uncover the identities, or that the complaint would be dismissed on other grounds.'" *Wakefield v. Thompson*, 177 F.3d 1160, 1163 (9th Cir. 1999) (alteration in original) (quoting *Gillespie v. Civiletti*, 629 F.2d 637, 642 (9th Cir. 1980)).

To determine whether a plaintiff has established good cause to seek the identity of a Doe defendant through expedited discovery, courts consider the following:

> whether the plaintiff (1) identifies the Doe defendant with sufficient specificity that the Court can determine that the defendant is a real person who can be sued in federal court, (2) recounts the steps taken to locate and identify the defendant, (3) demonstrates that the action can withstand a motion to dismiss, and (4) proves that the discovery

> is likely to lead to identifying information that will permit service of process.

ZG TOP Tech. Co. v. Doe, No. 19-cv-00092-RAJ, 2019 WL 917418, at *2 (W.D. Wash. Feb. 25, 2019) (citing *Bodyguard Prods., Inc. v. Doe 1*, 17-cv-01647-RSM, 2018 WL 1470873, at *1 (W.D. Wash. Mar. 26, 2018)); *see also Columbia Ins. Co. v. seescandy.com*, 185 F.R.D. 573, 578–80 (N.D. Cal. 1999).

DISCUSSION

Below, the court first analyzes whether plaintiff has met its burden under Rule 65(b)(1)(b) to justify the granting of an *ex parte* temporary restraining order in this case. The court then addresses whether plaintiff has met its burden of demonstrating an irreparable injury which would warrant the granting of the requested relief. Finally, the court considers whether plaintiff has adequately supported its request for the authorization of expedited discovery to attempt to discover the identities of Doe defendant(s).

A. Rule 65 Notice

As addressed above, a temporary restraining order may be issued without notice to the adverse party or its attorney only under strictly limited circumstances. Fed. R. Civ. P. 65(b)(1); *see also* L.R. 231(a) ("Except in the most *extraordinary of circumstances*, no temporary restraining order shall be granted in the absence of actual notice to the affected party and/or counsel, by telephone or other means, or a sufficient showing of efforts made to provide notice.") (emphasis added). The Supreme Court has emphasized, an *ex parte* temporary restraining order is justified only in very limited circumstances:

> The stringent restrictions imposed . . . by Rule 65 on the availability of ex parte temporary restraining orders reflect the fact that our entire jurisprudence runs counter to the notion of court action taken before reasonable notice and an opportunity to be heard has been granted both sides of a dispute. *Ex parte* temporary restraining orders are no doubt necessary in certain circumstances, but under federal law they should be restricted to serving their underlying purpose of preserving the status quo and preventing irreparable harm just so long as is necessary to hold a hearing, and no longer.

Granny Goose Foods, Inc., 415 U.S. at 438–39 (internal citation omitted); *McZeal v. EMC Mortg. Corp.*, No. 13-cv-07220-MMM-CW, 2013 WL 12138853, at *1 n. 3 (C.D. Cal. Nov. 4, 2013)

("Only in rare circumstances can a federal court issue a TRO without written or oral notice to the adverse party."). "In cases where notice could have been given to the adverse party, courts have recognized 'a very narrow band of cases in which *ex parte* orders are proper because notice to the defendant would render fruitless the further prosecution of the action.'" *Reno Air Racing Ass'n, Inc. v. McCord*, 452 F.3d 1126, 1131 (9th Cir. 2006) (quoting *Am. Can Co. v. Mansukhani*, 742 F.2d 314, 322 (7th Cir. 1984)); *see also Harnden v. Perez*, No. 21-cv-09231-LHK, 2021 WL 7367123, at *3 (N.D. Cal. Dec. 8, 2021).

Here, plaintiff's counsel has submitted an affidavit pursuant to Rule 65(b)(1)(b) stating that providing advance notice to defendants in this case would make it highly likely that they would move the assets at issue out of the reach of this court. (Doc. No. 2-3 at ¶ 4.) The court acknowledges that cryptocurrency such as that at issue here "poses a heightened risk of asset dissipation." *FTC v. Dluca*, No. 18-cv-60379-LSS, 2018 WL 1830800, at *2–3 (S.D. Fla. Feb. 28, 2018) ("[C]ryptocurrencies are circulated through a decentralized computer network, without relying on traditional banking institutions or other clearinghouses. This independence from traditional custodians makes it difficult for law enforcement to trace or freeze cryptocurrencies in the event of fraud or theft[]"), *report and recommendation adopted*, No. 18-cv-60379-KMM-LSS, 2018 WL 1811904 (S.D. Fla. Mar. 12, 2018). However, "a single conclusory statement by counsel about" what defendants may do is insufficient to meet the requirements of Rule 65(b)(1)(b). *Reno Air Racing Ass'n., Inc.*, 452 F.3d at 1132 ("Were a single conclusory statement by counsel about infringers sufficient to meet the dictates of Rule 65, then *ex parte* orders without notice would be the norm and this practice would essentially gut Rule 65's notice requirements."). Here, the bare statement by plaintiff's counsel that defendants are likely to immediately move the cryptocurrency assets at issue in this action through channels designed to prevent tracing of those assets is unsupported by evidence and is insufficient to justify the granting of *ex parte* relief. *See Nexon Am. Inc. v. GK*, No. 5:21-cv-00886-JWH, 2021 WL 9315450, at *3 (C.D. Cal. Sept. 2, 2021) (finding that the plaintiff's assertion that the defendants "most certainly will move assets to other accounts" upon notice was insufficient to support the issuance of an *ex parte* temporary restraining order).

To support its contention that defendants will immediately begin transferring assets, plaintiff also provides a declaration from Adam Zarazinski ("the Zarazinski declaration"), the CEO of a financial intelligence company who has developed expertise in financial data analysis, digital forensics, and cryptocurrency. (Doc. No. 2-2 at ¶¶ 2, 3.) The declaration was prepared after the declarant was hired by Opentensor to investigate the Bittensor attacks. (*Id.* at ¶ 6.) In it, Mr. Zarazinski indicates that defendants' actions are consistent with illicit actors in cryptocurrency fraud cases. (*Id.* at ¶ 38.) He declares that in his experience, "advance notice to cryptocurrency thieves of legal proceedings typically results in immediate attempts to move assets[.]" (*Id.* at ¶ 39.)

However, a plaintiff seeking *ex parte* relief on the basis that the adverse party will transfer assets must support that assertion by, for instance, showing that the adverse party has a history of disregarding court orders or that persons similar to the adverse party have such a history. *See Adobe Sys., Inc. v. S. Sun Prods., Inc.*, 187 F.R.D. 636, 640 (S.D. Cal. 1999) (discussing how, in order to justify proceeding *ex parte*, the plaintiff was required to show that the defendants would have disregarded a court order and destroyed evidence within the time it would take to hold a hearing) (citing *First Tech. Safety Sys., Inc. v. Depinet*, 11 F.3d 641, 650–51 (6th Cir. 1993)). Here, the Zarazinski declaration provides no support for any suggestion that the named defendants have a history of disobeying court orders, but rather states only that "cryptocurrency thieves" will immediately attempt to move assets upon notice of legal proceedings. (Doc. No. 2-2 at ¶ 39.) The Zarazinski declaration simply does not provide support for plaintiff's contention that those *accused* of stealing cryptocurrency will immediately attempt to transfer assets. *See Int'l Mkts. Live, Inc. v. Huss*, No. 2:20-cv-00866-JAD-BNW, 2020 WL 2559926, at *2 (D. Nev. May 20, 2020) (holding that the plaintiff did not meet the "demanding burden" to obtain *ex parte* relief where the plaintiff had not shown either that the defendant had a history of violating court orders or that persons in a similar situation have a history of violating court orders). Accordingly, the court concludes that plaintiff has not met its burden of showing that defendants would violate a court order and transfer assets if provided with the presumptively required notice.

/////

Plaintiff has not met its burden under Rule 65(b)(1)(b) of justifying the issuance of relief on an *ex parte* basis based on the declarations it has submitted to the court. The court will therefore deny plaintiff's *ex parte* motion for a temporary restraining order without prejudice to it renewing its motion upon providing notice to the adverse parties as required under Rule 65. Nevertheless, for the sake of efficiency, the court will analyze below whether plaintiff has sufficiently demonstrated a likelihood of irreparable harm that would justify the issuance of a temporary restraining order.

B. Irreparable Harm

The risk of irreparable harm must be "likely, not just possible." *All. for the Wild Rockies*, 632 F.3d at 1131. "Speculative injury does not constitute irreparable injury sufficient to warrant granting a preliminary injunction." *Caribbean Marine Servs. Co.*, 844 F.2d at 674.

Here, plaintiff argues that it has demonstrated a likelihood of irreparable harm because, should defendants be given advance notice, defendants "will likely . . . move assets through mixers, privacy protocols, or to unregulated exchanges in non-cooperative jurisdictions." (Doc. No. 2-1 at 18.) It asserts that such moves would likely make it impossible to compel return of the assets that are the subject of this action. (*Id.*) Based upon the Zarazinski declaration, plaintiff further asserts that defendants resumed stolen asset transfers on January 20, 2025, creating a risk of imminent asset dissipation. (*Id.*; Doc. No. 2-2 at ¶ 33.)

"The propriety of a TRO hinges on a significant threat of irreparable injury that must be imminent in nature." *Farmers Ins. Exch. v. Steele Ins. Agency*, No. 2:13-cv-00784-MCE-DAD, 2013 WL 1819988, at *1 (E.D. Cal. Apr. 30, 2013) (citing *Caribbean Marine Servs. Co.*, 844 F.2d at 674)); *see also Yamout v. Scapa*, No. 24-cv-08876-SVW-PD, 2024 WL 5185324, at *3–4 (C.D. Cal. Oct. 22, 2024) (finding that an unexplained delay of ten months in filing a motion seeking a temporary restraining order weighed against a finding of irreparable harm) (citing *Oakland Trib., Inc. v. Chron. Publ'g Co.*, 762 F.2d 1374, 1377 (9th Cir. 1985)). Notable here is that neither plaintiff, nor its assignor of rights Nakamoto, sought a temporary restraining order until January 27, 2025, despite discovery of the alleged cyberattacks on July 3, 2024. (Doc. No. 2-1 at 9.) Seemingly addressing the issue of plaintiff's delay, Mr. Zarazinski declares that on

January 20, 2025, two of the Destination Addresses began transferring assets after a period of inactivity that began in July 2024. (Doc. No. 2-2 at ¶ 33); *see Stephens v. Doe*, No. 23-cv-04183-JD, 2023 WL 5988592, at *1 (N.D. Cal. Sept. 13, 2023) (finding that, when the plaintiff had waited more than 90 days to request a temporary restraining order and offered no evidence that the targeted assets were being transferred, there was no pressing need for a TRO). The Zarazinski declaration also states that consolidation of assets into certain digital wallets for extended periods followed by sudden transfers is common in cryptocurrency fraud cases, which heightens the risk of imminent dissipation of funds. (Doc. No. 2-2 at ¶ 38.) Based on this opinion, plaintiffs argue that the risk of further asset dissipation is imminent due to the typical behavior of cryptocurrency thieves. (Doc. No. 2-1 at 18.)

This court has previously recognized that under certain circumstances the risk of irreparable harm is heightened in the context of fraudulent transfers of cryptocurrency due to the risk of asset dissipation. *See Jacobo v. Doe*, No. 1:22-cv-00672-DAD-BAK, 2022 WL 2052637, at *5 (E.D. Cal. June 7, 2022); *Gaponyuk v. Alferov*, No. 2:23-cv-01317-KJM-JDP, 2023 WL 4670043, at *3 (E.D. Cal. July 20, 2023) (noting that cryptocurrency transactions can be untraceable and anonymous creating risks of asset dissipation); *see also Yogaratnam v. Dubois*, No. 24-cv-00393-NJB, 2024 WL 758387, at *4 (E.D. La. Feb. 23, 2024) (finding that the plaintiff in that case had made a showing of irreparable harm because the defendants could transfer allegedly stolen assets to inaccessible digital wallets at any moment).

However, other district courts have concluded that the issuance of a temporary restraining order is generally inappropriate in cases involving the alleged theft of cryptocurrency where monetary damages were available and would suffice. *See Newton AC/DC Fund L.P. v. Hector DAO*, No. 24-cv-00722-RK-JBD, 2024 WL 580182, at *3–4 (D.N.J. Feb. 13, 2024) (holding that, where the plaintiff did not make a showing that the defendants were likely unable to pay an award of money damages, the plaintiff had not shown irreparable injury justifying injunctive relief); *see also Schiermeyer ex rel. Blockchain Game Partners, Inc. v. Thurston*, 697 F. Supp. 3d 1265, 1272–73 (D. Utah 2023) (finding that, because cryptocurrency tokens are "fungible and easy to value," the plaintiff had failed to make an adequate showing of imminent irreparable harm

because he had not demonstrated that the defendant would be unable to pay an award of monetary damages); *MacDonald v. Dynamic Ledger Sols., Inc.*, No. 17-cv-07095-RS, 2017 WL 6513439, at *3 (N.D. Cal. Dec. 20, 2017) (finding that the plaintiff had not shown an immediate risk of irreparable harm where it was unclear that damages would be inadequate to compensate the plaintiff). In making the determination of whether monetary damages are actually available and therefore would provide sufficient relief in cryptocurrency fraud cases, courts have looked to factors such as whether the defendants' identities are known, whether the fraudulent scheme is ongoing, and the defendants' conduct in the litigation. *See Blum v. Tara*, No. 3:23-cv-24734-MCR-HTC, 2024 WL 5317287, at *4 (N.D. Fla. Feb. 5, 2024) (collecting cases in the context of a permanent injunction and finding irreparable injury was demonstrated where the defendants had defaulted and appeared to intend to continue a fraudulent scheme); *Bullock v. Doe*, No. 23-cv-03041-CJW-KEM, 2023 WL 9503380, at *5 (N.D. Iowa Nov. 3, 2023) (finding that where the identity of the defendants was unknown and the cryptocurrency assets could be quickly transferred that plaintiff had demonstrated irreparable injury).

Based on their delay in filing this action and the pending motion for emergency relief as well as their failure to show that monetary damages are likely to be unavailable or otherwise insufficient, the court believes plaintiff has not at this time met its burden of demonstrating a likelihood of irreparable harm absent the granting of the requested relief. In the present case, plaintiff's Zarazinski declaration indicates that the Bittensor cyberattacks began seven months prior to the filing of plaintiff's request for a temporary restraining order and six months prior to the discovery by Opentensor of the Bittensor attacks, though it does not state when the assets stolen in the attacks were traced to the Destination Addresses. (Doc. No. 2-2 at ¶¶ 13, 17.) Mr. Zarazinski also declares that after the Bittensor attacks, the attackers transferred assets to the Destination Addresses, but he does not state when those transfers occurred other than the transfers received by two specific Destination Addresses on July 3, 2024. (*Id.* at ¶ 33.) Though plaintiff's investigation has apparently revealed that some assets of unknown origin were transferred on January 20, 2025, this is not an adequate basis upon which to find a risk of "imminent" injury based on the comparatively small volume of asset transfers to the amount allegedly taken in the

Bittensor attacks and the months-long delay in seeking emergency relief. *See Stephens*, 2023 WL 5988592, at *1 (holding that the plaintiff had not demonstrated imminent irreparable injury where 95 percent of the assets at issue were sitting undisturbed in digital wallets for 90 days). Plaintiff has also failed to allege that the named defendants would be unable to pay an award of monetary damages should it prevail in this case. *See Schiermeyer*, 697 F. Supp. 3d at 1273 (holding that, because the stolen cryptocurrency was fungible, the plaintiff must demonstrate that the defendant was likely to be unable to pay an award of monetary damages to demonstrate a likelihood of irreparable harm); *Bandyopadhyay v. Defendant 1*, No. 22-cv-22907-BB, 2023 WL 2263552, at *5–7 (S.D. Fla. Feb. 28, 2023) (holding, in a cryptocurrency fraud context, that the plaintiff had not shown irreparable injury where the plaintiff had not shown monetary damages would not compensate him for his loss); *see also Cal. Pharmacists Ass'n v. Maxwell-Jolly*, 563 F.3d 847, 851–52 (9th Cir. 2009) ("Typically, monetary harm does not constitute irreparable harm. . . . [E]conomic damages are not traditionally considered irreparable because the *injury can later be remedied by a damage award*.") (emphasis in original), *vacated on other grounds by Douglas v. Indep. Living Ctr. of S. Cal., Inc.*, 565 U.S. 606 (2012).

Other factors relied upon by courts as weighing in favor of granting injunctive relief in somewhat similar cases are also absent here. Though the risks of asset dissipation in the cryptocurrency context may be heightened, particularly when a "plaintiff has been unable to identify the people behind the alleged scheme," plaintiff in this case has identified and named three defendants. *Bullock*, 2023 WL 9503380, at *5 (finding that the likelihood the defendants would move cryptocurrency assets out of the plaintiff's reach was heightened where the defendants' identities were unknown). Unlike in a previous case before the undersigned, there is no indication here that defendants have begun liquidating cryptocurrency assets. *See Jacobo*, 2022 WL 2052637, at *1–2 (describing the plaintiff's allegations that the unidentified defendant may have begun liquidating assets); *see also Leidel v. Project Invs., Inc.*, No. 9:16-cv-80060-KAM, 2021 WL 4991325, at *2 (S.D. Fla. May 28, 2021) (finding that the plaintiff had shown the likelihood of irreparable injury where the defendant had begun to liquidate stolen assets). Because the identity of at least some defendants are known and the assets at issue have remained

static for an extended period, it would appear that plaintiff must make some showing that those defendants are likely to be unable to pay an award of damages were plaintiff to prevail in this action. *See Newton AC/DC Fund L.P.*, 2024 WL 580182, at *3 (finding that the plaintiff had not shown irreparable injury when it had not shown that the identified defendants would be unable to pay an award of damages).

Finally, even if plaintiff had met its burden of demonstrating irreparable harm, the court must ensure that the injunctive relief sought is targeted at preventing the irreparable injury present, specifically the dissipation of assets that its assignor owns. *See, e.g.*, *Stephens*, 2023 WL 5988592, at *2 (denying a request for a temporary restraining order where the plaintiff did not demonstrate that the listed accounts contained only assets that he purportedly owned); *Huntley v. VBit Techs. Corp.*, No. 22-cv-01164-CFC-SRF, 2023 WL 5938665, at *4–5 (D. Del. Aug. 10, 2023) (finding that, where the evidence showed that certain wallets held assets owned by numerous individuals, the plaintiff was required to show that the extraordinary remedy of imposing a prejudgment freeze on those wallets was necessary in order to prevent irreparable harm), *report and recommendation adopted*, No. 22-cv-01164-CFC-SRF, 2023 WL 5932946 (D. Del. Sept. 12, 2023). Here, plaintiff contends that the tokens valued at $13,000,000 it alleges were stolen from its assignor were taken during the June 1 cyberattack. (Doc. No. 2-1 at 9.) Plaintiff also provides a list of the Destination Addresses of the assets taken in that attack. (Doc. Nos. 1 at ¶ 54; 2-2 at ¶ 18.) However, plaintiff has not presented any evidence that those Destination Addresses contain only assets which were stolen from its assignor in the June 1 attack. Indeed, the Zarazinski declaration indicates that some of the assets taken during that cyberattack were put into the Binance exchange, which uses an omnibus account system that pools funds from multiple users into shared wallets. (Doc. No. 2-2 at ¶¶ 18, 36.) Freezing of the assets contained in the Destination Addresses associated with such a system would clearly appear to impact nonparties to this litigation, since nonparties may well have had their assets pooled into the same digital wallets as the assets at issue in this case. *See Huntley*, 2023 WL 5938665, at *5 (denying the request for the extraordinary remedy of freezing assets where the plaintiffs did not show that the assets being frozen were controlled by the defendants). Therefore, the court

concludes that plaintiff has not met its burden of showing that the emergency relief it seeks is appropriate to prevent the harm that plaintiff contends it will suffer. *See, e.g., Montes v. U.S. Bank N.A.*, 10-cv-00022-PSG-JC, 2010 WL 11597574, at *2 (C.D. Cal. Jan. 12, 2010) (denying a request for temporary restraining order on the basis that the plaintiff failed to meet its burden to show a likelihood of irreparable injury); *Vigneron Partners, LLC v. Woop Woop Wines Pty Ltd.*, No. 06-cv-00527-JF, 2006 WL 8460096 (N.D. Cal. Mar. 31, 2006) (same).

If plaintiff were to renew its motion for a temporary restraining order after providing the required notice, it is directed to also address the deficiencies noted in this order with respect to its showing of irreparable harm.

C. Expedited Discovery[8]

Plaintiff also seeks to expedite discovery to attempt to identify unknown defendants. (Doc. No. 2-1 at 21.) To that end, plaintiff argues that it has demonstrated good cause to seek the identity of these unknown defendants based on its pending request for a temporary restraining order and the narrow tailoring of its proposed discovery request. (*Id.* at 22.) Plaintiff contends it can discover these identities through third-party subpoenas directed to the cryptocurrency exchanges Coinbase, Binance, Whitebit, eXch, Kucoin, HTX, MexC, Elolix, Kraken, and OKX (collectively "the Exchanges"). (*Id.* at 23.) In particular, plaintiff seeks to obtain:

> [C]urrently unavailable transaction histories from May 1, 2024 (approximately 1 month before the attack) until the present, including (1) records of deposits and withdrawals; (2) records of transfers to/from identified wallet addresses; (3) information about source and destination of funds; and (4) records of currency conversions or swaps.
>
> With respect to the identity of unknown defendants, Plaintiff intends to seek narrowly tailored information including (1) account opening and closing documents; (2) Know Your Customer (KYC) and Anti-Money Laundering (AML) verification materials; (3) government-issued identification documents; (4) proof of address documentation; and (5) information about beneficial owners and authorized users.

[8] The undersigned is addressing plaintiff's motion for expedited discovery in this order because of its inclusion with the *ex parte* application for a temporary restraining order. However, the undersigned notes that any future motions pertaining to discovery, including those related to expedited discovery, are to be properly noticed before the assigned magistrate judge in accordance with Local Rule 302(c)(1). L.R. 302.

(*Id.* at 23–24.)

"In the Ninth Circuit, courts use the 'good cause' standard to determine whether discovery should be allowed to proceed prior to a Rule 26(f) conference." *Rovio Ent. Ltd.*, 907 F. Supp. 2d at 1099. As noted above, "[i]n considering whether good cause exists, factors courts may consider include: (1) whether a preliminary injunction is pending; (2) the breadth of the discovery request; (3) the purpose for requesting the expedited discovery; (4) the burden on the defendants to comply with the requests; and (5) how far in advance of the typical discovery process the request was made." *Id.* (citing *Am. LegalNet, Inc. v. Davis*, 673 F. Supp. 2d 1063, 1067 (C.D. Cal. 2009)).

In this case, plaintiff has diligently sought out the identities of the unknown defendant(s) by employing a cryptocurrency investigator to identify the accounts to which its assignor's assets were transferred. (Doc. No. 2-2 at ¶¶ 2–4) (describing the qualifications of plaintiff's investigator); *see Lee v. Does #1-3*, No. 2:23-cv-02008, 2024 WL 472375, at *1 (W.D. Wash. Jan. 10, 2024) (holding that the plaintiff had shown good cause for expedited discovery as to the identity of the unknown defendants where diligence was shown by the hiring of a cryptocurrency investigator). As discussed above, plaintiff has recounted in its motion and attached declarations the steps it has taken to trace the destinations and the specific wallet addresses the allegedly stolen assets are currently in. "Courts routinely allow early discovery for the limited purpose of identifying defendants on whom process could not otherwise be served, which is precisely Plaintiff['s] intent here." *Amazon.com, Inc. v. Does 1-20*, No. 2:24-cv-01083-TL, 2024 WL 4893384, at *2 (W.D. Wash. Nov. 26, 2024) (internal quotation marks omitted) (quoting *Amazon.com, Inc. v. Dafang Haojiafu Hotpot Store*, No. 2:21-cv-00766-RSM, 2022 WL 2511742, at *2 (W.D. Wash. June 8, 2022)). Accordingly, the court will grant plaintiff's request for expedited discovery directed to the above-listed cryptocurrency exchanges solely for the purpose of obtaining identifying information about the unknown defendant(s). Upon service of a Rule 45 subpoena to the Exchanges, defendants or the Exchanges will have an opportunity to raise objections through a motion to quash in which they could attempt to demonstrate to the court that prejudice to them outweighs plaintiff's need for the information sought.

However, the court does not find that plaintiff has narrowly tailored all of its proposed discovery requests to the cryptocurrency exchanges or provided good cause for the authorizing of expedited discovery beyond specific identifying information about the Doe defendant. In particular, plaintiff's proposed discovery requests for documents and information regarding transactions involving the Destination Addresses and communication with defendant and any non-party accountholder of the Destination Addresses appears to "seek affirmative relief from this [c]ourt that is the subject of this lawsuit, and go[es] well beyond the request for expedited discovery." *See ZG TOP Tech. Co.*, 2019 WL 917418, at *3. Other district courts in this circuit have declined to broaden the scope of expedited discovery to transaction information, even when a plaintiff contends, as plaintiff does here, that it needs this information to prevent asset dissipation. *See Lee*, 2024 WL 472375, at *2 (finding that the potential harms to the defendants of exposing sensitive account information outweighed the risk of loss to the plaintiff); *Kovalenko v. Does 1-5*, No. 2:22-cv-01578-TL, 2022 WL 17582483, at *3 (W.D. Wash. Dec. 12, 2022) (authorizing expedited discovery for the limited purpose of identifying the defendants but not as to discovery of cryptocurrency wallet addresses and transaction numbers).

Accordingly, the court will deny authorization of discovery requests not targeted at the identities of the unknown defendants on an expedited basis.

CONCLUSION

For the reasons explained above, plaintiff's motion for a temporary restraining order is denied and plaintiff's motion for expedited discovery is granted in part (Doc. No. 2) as follows:

1. Plaintiff's motion for a temporary restraining order is denied without prejudice to refiling with proper notice;
2. Plaintiff's motion for expedited discovery is granted in part as follows:
    a. Plaintiff may immediately serve a Rule 45 subpoena on the Exchanges seeking the following information about the owners and authorized users of the Destination Addresses (the unknown defendant(s)): legal name, street address, telephone number, and email address. It may not include defendants' social security numbers. A copy of this order shall be attached

to the subpoena;

i. If a cryptocurrency exchange is served with a subpoena authorized by this order, it shall serve a copy of the subpoena and a copy of this order to the defendant and any other affected user as soon as possible after service of the subpoena. The cryptocurrency exchange may serve the user using any reasonable means, including written notice sent to the user's last known address, transmitted either by first-class mail or via overnight service. The cryptocurrency exchange shall provide plaintiff with the date when such notice was provided to any affected user;

ii. The cryptocurrency exchanges and any affected user shall have fourteen (14) days from the respective date of service of the subpoena upon them to object to the subpoena pursuant to Federal Rule of Civil Procedure 45(d)(2)(B);

iii. The cryptocurrency exchanges shall not disclose the identifying information of the owners and authorized users of the Destination Addresses, or such information for any other affected user, during the 14-day period or if a timely objection is served unless and until the Court orders it to do so;

iv. If an objection is served, the cryptocurrency exchanges shall preserve any material responsive to the subpoena for a period of no less than ninety (90) days in order to allow plaintiff to move for an order compelling production under Federal Rule of Civil Procedure 45(d)(2)(B)(i); and

v. If no objection is served, the cryptocurrency exchanges shall comply with the subpoena within twenty-one (21) days of service;

/////

/////

b. Plaintiff's motion for expedited discovery (Doc. No. 2) is denied as to all its other proposed discovery requests.

IT IS SO ORDERED.

Dated: **February 7, 2025**

DALE A. DROZD
UNITED STATES DISTRICT JUDGE